

ABSTRACT OF THE DISCLOSURE

A method and apparatus for secure data transmission via network. Transmission side transmits processed data, second signed data obtained by applying one-way function to merged data of the processed data and first signed data of an original image and ciphering the output of the one-way function with transmission side secret key, and ciphered signed data obtained by ciphering the first signed data with reception side private key. Data reception side enciphers received ciphered signed data with reception side secret key to obtain third signed data, applies one-way function to merged data of received processed data and the third signed data, enciphers received second signed data with transmission side private key, compares result obtained by applying the one-way function to the merged data with result obtained by enciphering the second signed data for data validation.